



StorageGRID 네트워크 및 연결 관리

StorageGRID 11.5

NetApp
April 11, 2024

목차

StorageGRID 네트워크 및 연결 관리	1
StorageGRID 네트워크 지침	1
IP 주소 보기	2
발신 TLS 연결에 지원되는 암호	3
네트워크 전송 암호화를 변경하는 중입니다	4
서버 인증서를 구성하는 중입니다	5
스토리지 프록시 설정을 구성하는 중입니다	11
관리자 프록시 설정을 구성합니다	13
트래픽 분류 정책 관리	14
링크 비용은 얼마입니까	27

StorageGRID 네트워크 및 연결 관리

그리드 관리자를 사용하여 StorageGRID 네트워크 및 연결을 구성하고 관리할 수 있습니다.

을 참조하십시오 ["S3 및 Swift 클라이언트 연결 구성"](#) S3 또는 Swift 클라이언트를 연결하는 방법에 대해 알아보십시오.

- ["StorageGRID 네트워크 지침"](#)
- ["IP 주소 보기"](#)
- ["발신 TLS 연결에 지원되는 암호"](#)
- ["네트워크 전송 암호화를 변경하는 중입니다"](#)
- ["서버 인증서를 구성하는 중입니다"](#)
- ["스토리지 프록시 설정을 구성하는 중입니다"](#)
- ["관리자 프록시 설정을 구성합니다"](#)
- ["트래픽 분류 정책 관리"](#)
- ["링크 비용은 얼마입니까?"](#)

StorageGRID 네트워크 지침

StorageGRID는 그리드 노드당 최대 3개의 네트워크 인터페이스를 지원하므로 각 개별 그리드 노드의 네트워킹을 보안 및 액세스 요구 사항에 맞게 구성할 수 있습니다.



그리드 노드의 네트워크를 수정하거나 추가하려면 복구 및 유지 관리 지침을 참조하십시오. 네트워크 토폴로지에 대한 자세한 내용은 네트워킹 지침을 참조하십시오.

그리드 네트워크

필수 요소입니다. 그리드 네트워크는 모든 내부 StorageGRID 트래픽에 사용됩니다. 그리드에서 모든 사이트 및 서브넷의 모든 노드 간에 연결을 제공합니다.

관리자 네트워크

선택 사항. 관리 네트워크는 일반적으로 시스템 관리 및 유지 보수에 사용됩니다. 클라이언트 프로토콜 액세스에도 사용할 수 있습니다. 관리 네트워크는 일반적으로 사설 네트워크이며 사이트 간에 라우팅할 필요가 없습니다.

클라이언트 네트워크

선택 사항. 클라이언트 네트워크는 일반적으로 S3 및 Swift 클라이언트 애플리케이션에 대한 액세스를 제공하는 데 사용되는 개방형 네트워크이므로 그리드 네트워크를 격리하고 보호할 수 있습니다. 클라이언트 네트워크는 로컬 게이트웨이를 통해 연결할 수 있는 모든 서브넷과 통신할 수 있습니다.

지침

- 각 StorageGRID 그리드 노드에는 할당된 각 네트워크에 대한 전용 네트워크 인터페이스, IP 주소, 서브넷 마스크 및 게이트웨이가 필요합니다.

- 그리드 노드는 네트워크에 둘 이상의 인터페이스를 가질 수 없습니다.
- 네트워크 당, 그리드 노드별로 단일 게이트웨이가 지원되며 노드와 동일한 서브넷에 있어야 합니다. 필요한 경우 게이트웨이에서 보다 복잡한 라우팅을 구현할 수 있습니다.
- 각 노드에서 각 네트워크는 특정 네트워크 인터페이스에 매핑됩니다.

네트워크	인터페이스 이름입니다
그리드	eth0
관리자(선택 사항)	eth1
클라이언트(선택 사항)	eth2

- 노드가 StorageGRID 어플라이언스에 연결된 경우 각 네트워크에 대해 특정 포트가 사용됩니다. 자세한 내용은 어플라이언스 설치 지침을 참조하십시오.
- 기본 라우트는 노드당 자동으로 생성됩니다. eth2가 활성화된 경우 0.0.0.0/0 은 eth2의 클라이언트 네트워크를 사용합니다. eth2가 활성화되지 않은 경우 0.0.0.0/0 은 eth0의 그리드 네트워크를 사용합니다.
- 그리드 노드가 그리드에 가입될 때까지 클라이언트 네트워크가 작동하지 않습니다
- 그리드 노드를 구축하는 동안 관리 네트워크를 구성하여 그리드를 완전히 설치하기 전에 설치 사용자 인터페이스에 액세스할 수 있습니다.

관련 정보

["유지 및 복구"](#)

["네트워크 지침"](#)

IP 주소 보기

StorageGRID 시스템의 각 그리드 노드에 대한 IP 주소를 볼 수 있습니다. 그런 다음 이 IP 주소를 사용하여 명령줄에서 그리드 노드에 로그인하고 다양한 유지보수 절차를 수행할 수 있습니다.

필요한 것

지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.

이 작업에 대해

IP 주소 변경에 대한 자세한 내용은 복구 및 유지 관리 지침을 참조하십시오.

단계

1. 노드 * > *GRID node * > * Overview * 를 선택합니다.
2. IP 주소 제목 오른쪽에 있는 * 더 보기 * 를 클릭합니다.

해당 그리드 노드의 IP 주소가 테이블에 나열됩니다.

Node Information ⓘ

Name SGA-lab11
Type Storage Node
ID 0b583829-6659-4c6e-b2d0-31461d22ba67

Connection State ✔ Connected
Software Version 11.4.0 (build 20200527.0043.61839a2)
IP Addresses 192.168.4.138, 10.224.4.138, 169.254.0.1 [Show less](#) ▲

Interface	IP Address
eth0	192.168.4.138
eth0	fd20:331:331:0:2a0:98ff:fea1:831d
eth0	fe80::2a0:98ff:fea1:831d
eth1	10.224.4.138
eth1	fd20:327:327:0:280:e5ff:fe43:a99c
eth1	fd20:8b1e:b255:8154:280:e5ff:fe43:a99c
eth1	fe80::280:e5ff:fe43:a99c
hic2	192.168.4.138
hic4	192.168.4.138
mtc1	10.224.4.138
mtc2	169.254.0.1

관련 정보

["유지 및 복구"](#)

발신 TLS 연결에 지원되는 암호

StorageGRID 시스템은 ID 페더레이션 및 클라우드 스토리지 풀에 사용되는 외부 시스템에 대한 TLS(Transport Layer Security) 연결을 위한 제한된 암호화 그룹 세트를 지원합니다.

지원되는 TLS 버전입니다

StorageGRID는 ID 페더레이션 및 클라우드 스토리지 풀에 사용되는 외부 시스템에 대한 연결을 위해 TLS 1.2 및 TLS 1.3을 지원합니다.

외부 시스템과 호환되도록 외부 시스템에 사용할 수 있도록 지원되는 TLS 암호가 선택되었습니다. 이 목록은 S3 또는 Swift 클라이언트 애플리케이션에서 사용할 수 있도록 지원되는 암호화 목록보다 큼니다.



프로토콜 버전, 암호, 키 교환 알고리즘 및 MAC 알고리즘과 같은 TLS 구성 옵션은 StorageGRID에서 구성할 수 없습니다. 이러한 설정에 대한 구체적인 요청이 있을 경우 NetApp 어카운트 담당자에게 문의하십시오.

지원되는 TLS 1.2 암호 그룹

지원되는 TLS 1.2 암호 제품군은 다음과 같습니다.

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_with_CHACH20_POLY1305
- TLS_ECDHE_ECDSA_WITH_CHACH20_POLY1305
- TLS_RSA_with_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384

지원되는 TLS 1.3 암호 그룹

지원되는 TLS 1.3 암호 제품군은 다음과 같습니다.

- TLS_AES_256_GCM_SHA384
- TLS_CHACH20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256

네트워크 전송 암호화를 변경하는 중입니다

StorageGRID 시스템은 TLS(Transport Layer Security)를 사용하여 그리드 노드 간의 내부 제어 트래픽을 보호합니다. 네트워크 전송 암호화 옵션은 TLS가 그리드 노드 간의 제어 트래픽을 암호화하는 데 사용하는 알고리즘을 설정합니다. 이 설정은 데이터 암호화에 영향을 주지 않습니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.

이 작업에 대해

기본적으로 네트워크 전송 암호화는 AES256-SHA 알고리즘을 사용합니다. AES128-SHA 알고리즘을 사용하여 제어 트래픽을 암호화할 수도 있습니다.

단계

1. 구성 * * 시스템 설정 * 그리드 옵션 * 을 선택합니다.
2. 네트워크 옵션 섹션에서 네트워크 전송 암호화를 * AES128-SHA * 또는 * AES256-SHA * (기본값)로 변경합니다.

Network Options



3. 저장 * 을 클릭합니다.

서버 인증서를 구성하는 중입니다

StorageGRID 시스템에서 사용하는 서버 인증서를 사용자 지정할 수 있습니다.

StorageGRID 시스템은 다음과 같은 여러 가지 목적으로 보안 인증서를 사용합니다.

- 관리 인터페이스 서버 인증서: 그리드 관리자, 테넌트 관리자, 그리드 관리 API 및 테넌트 관리 API에 대한 액세스를 보호하는 데 사용됩니다.
- 스토리지 API 서버 인증서: API 클라이언트 애플리케이션이 객체 데이터를 업로드 및 다운로드하는 데 사용하는 스토리지 노드 및 게이트웨이 노드에 대한 액세스를 보호하는 데 사용됩니다.

설치 중에 생성된 기본 인증서를 사용하거나 이러한 기본 인증서 유형 중 하나 또는 둘 다를 사용자 지정 인증서로 바꿀 수 있습니다.

지원되는 유형의 사용자 지정 서버 인증서

StorageGRID 시스템은 RSA 또는 ECDSA(Elliptic Curve Digital Signature Algorithm)로 암호화된 사용자 지정 서버 인증서를 지원합니다.

StorageGRID가 REST API용 클라이언트 연결을 보호하는 방법에 대한 자세한 내용은 S3 또는 Swift 구현 가이드를 참조하십시오.

로드 밸런서 끝점용 인증서

StorageGRID는 로드 밸런서 끝점에 사용되는 인증서를 별도로 관리합니다. 로드 밸런서 인증서를 구성하려면 로드 밸런서 끝점을 구성하는 지침을 참조하십시오.

관련 정보

["S3을 사용합니다"](#)

["Swift를 사용합니다"](#)

["부하 분산 장치 엔드포인트 구성"](#)

Grid Manager 및 테넌트 관리자에 대한 사용자 지정 서버 인증서 구성

기본 StorageGRID 서버 인증서를 단일 사용자 지정 서버 인증서로 교체하여 보안 경고가 발생하지 않고 사용자가 그리드 관리자 및 테넌트 관리자에 액세스할 수 있도록 할 수 있습니다.

이 작업에 대해

기본적으로 모든 관리 노드에는 그리드 CA에서 서명한 인증서가 발급됩니다. 이러한 CA 서명 인증서는 하나의 공통 사용자 지정 서버 인증서 및 해당 개인 키로 대체할 수 있습니다.

단일 사용자 지정 서버 인증서가 모든 관리 노드에 사용되므로 클라이언트가 Grid Manager 및 Tenant Manager에 연결할 때 호스트 이름을 확인해야 하는 경우 인증서를 와일드카드 또는 다중 도메인 인증서로 지정해야 합니다. 사용자 지정 인증서를 정의하여 그리드의 모든 관리 노드와 일치시킵니다.

서버에서 구성을 완료해야 하며 사용 중인 루트 CA(인증 기관)에 따라 사용자가 그리드 관리자 및 테넌트 관리자에 액세스하는 데 사용할 웹 브라우저에 루트 CA 인증서를 설치해야 할 수도 있습니다.



실패한 서버 인증서로 인해 작업이 중단되지 않도록 하려면 이 서버 인증서가 만료될 때 * Management Interface * 용 서버 인증서 만료 알림과 레거시 관리 인터페이스 인증서 만료(MCEP) 경보가 모두 트리거됩니다. 필요에 따라 * 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택하여 현재 서비스 인증서가 만료될 때까지 일 수를 확인할 수 있습니다. 그런 다음 * 기본 관리 노드 * > * CMN * > * 리소스 * 를 선택합니다.



IP 주소 대신 도메인 이름을 사용하여 Grid Manager 또는 Tenant Manager에 액세스하는 경우, 다음 중 하나가 발생할 경우 브라우저에 인증서 오류가 표시되지 않고 무시하도록 옵션이 표시되지 않습니다.

- 사용자 지정 관리 인터페이스 서버 인증서가 만료됩니다.
- 사용자 지정 관리 인터페이스 서버 인증서를 기본 서버 인증서로 되돌립니다.

단계

1. 구성 * > * 네트워크 설정 * > * 서버 인증서 * 를 선택합니다.
2. 관리 인터페이스 서버 인증서 섹션에서 * 사용자 정의 인증서 설치 * 를 클릭합니다.
3. 필요한 서버 인증서 파일을 업로드합니다.
 - * 서버 인증서 *: 사용자 정의 서버 인증서 파일 (.crt)를 클릭합니다.
 - * 서버 인증서 개인 키 *: 사용자 지정 서버 인증서 개인 키 파일입니다 (.key)를 클릭합니다.



EC 개인 키는 224비트 이상이어야 합니다. RSA 개인 키는 2048비트 이상이어야 합니다.

- * CA 번들 *: 각 중간 발급 CA(인증 기관)의 인증서를 포함하는 단일 파일입니다. 파일에는 인증서 체인 순서에 연결된 PEM 인코딩된 CA 인증서 파일이 각각 포함되어야 합니다.

4. 저장 * 을 클릭합니다.

사용자 지정 서버 인증서는 이후의 모든 새 클라이언트 연결에 사용됩니다.

기본 StorageGRID 서버 인증서 또는 업로드된 CA 서명 인증서에 대한 자세한 정보를 표시하려면 탭을 선택합니다.



새 인증서를 업로드한 후 관련 인증서 만료 알림(또는 레거시 알람)이 지워지도록 최대 1일을 허용합니다.

5. 페이지를 새로 고쳐 웹 브라우저가 업데이트되도록 합니다.

Grid Manager 및 Tenant Manager에 대한 기본 서버 인증서 복원

Grid Manager 및 Tenant Manager에 대한 기본 서버 인증서를 사용하도록 되돌릴 수 있습니다.

단계

1. 구성 * > * 네트워크 설정 * > * 서버 인증서 * 를 선택합니다.
2. 인터페이스 서버 인증서 관리 섹션에서 * 기본 인증서 사용 * 을 클릭합니다.
3. 확인 대화 상자에서 * 확인 * 을 클릭합니다.

기본 서버 인증서를 복원하면 구성된 사용자 지정 서버 인증서 파일이 삭제되고 시스템에서 복구할 수 없습니다.

이후의 모든 새 클라이언트 연결에 기본 서버 인증서가 사용됩니다.

4. 페이지를 새로 고쳐 웹 브라우저가 업데이트되도록 합니다.

스토리지 노드 또는 **CLB** 서비스에 연결하기 위한 사용자 지정 서버 인증서 구성

스토리지 노드에 대한 S3 또는 Swift 클라이언트 연결에 사용되는 서버 인증서 또는 게이트웨이 노드의 CLB 서비스(더 이상 사용되지 않음)를 교체할 수 있습니다. 교체 사용자 지정 서버 인증서는 조직에 따라 다릅니다.

이 작업에 대해

기본적으로 모든 스토리지 노드에는 그리드 CA에서 서명한 X.509 서버 인증서가 발급됩니다. 이러한 CA 서명 인증서는 하나의 공통 사용자 지정 서버 인증서 및 해당 개인 키로 대체할 수 있습니다.

단일 사용자 지정 서버 인증서가 모든 스토리지 노드에 사용되므로 클라이언트가 스토리지 끝점에 연결할 때 호스트 이름을 확인해야 하는 경우 인증서를 와일드카드 또는 다중 도메인 인증서로 지정해야 합니다. 사용자 지정 인증서를 정의하여 그리드의 모든 스토리지 노드와 일치시킵니다.

서버에서 구성을 완료한 후 사용하는 루트 CA(인증 기관)에 따라 시스템에 액세스하는 데 사용할 S3 또는 Swift API 클라이언트에 루트 CA 인증서를 설치해야 할 수도 있습니다.



실패한 서버 인증서로 인해 작업이 중단되지 않도록 하려면 * Storage API Endpoints * 용 서버 인증서 만료 알림과 레거시 Storage API Service Endpoints 인증서 만료(SCEP) 경보가 모두 루트 서버 인증서가 만료될 때 트리거됩니다. 필요에 따라 * Support * * * Tools * * Grid Topology * 를 선택하여 현재 서비스 인증서가 만료될 때까지 일 수를 확인할 수 있습니다. 그런 다음 *기본 관리 노드 * * CMN * * 리소스 * 를 선택합니다.

사용자 지정 인증서는 클라이언트가 게이트웨이 노드에서 더 이상 사용되지 않는 CLB 서비스를 사용하여 StorageGRID에 연결하거나 스토리지 노드에 직접 연결하는 경우에만 사용됩니다. 관리 노드 또는 게이트웨이 노드에서 로드 밸런서 서비스를 사용하여 StorageGRID에 연결하는 S3 또는 Swift 클라이언트는 로드 밸런서 끝점에 대해 구성된 인증서를 사용합니다.



곧 만료되는 로드 밸런서 끝점에 대해 * 로드 밸런서 끝점 인증서 만료 * 경고가 트리거됩니다.

단계

1. 구성 * > * 네트워크 설정 * > * 서버 인증서 * 를 선택합니다.
2. 개체 스토리지 API 서비스 끝점 서버 인증서 섹션에서 * 사용자 지정 인증서 설치 * 를 클릭합니다.
3. 필요한 서버 인증서 파일을 업로드합니다.
 - * 서버 인증서 *: 사용자 정의 서버 인증서 파일 (.crt)를 클릭합니다.
 - * 서버 인증서 개인 키 *: 사용자 지정 서버 인증서 개인 키 파일입니다 (.key)를 클릭합니다.



EC 개인 키는 224비트 이상이어야 합니다. RSA 개인 키는 2048비트 이상이어야 합니다.

- * CA 번들 *: 각 중간 발급 CA(인증 기관)의 인증서를 포함하는 단일 파일입니다. 파일에는 인증서 체인 순서에 연결된 PEM 인코딩된 CA 인증서 파일이 각각 포함되어야 합니다.

4. 저장 * 을 클릭합니다.

사용자 지정 서버 인증서는 이후의 모든 새 API 클라이언트 연결에 사용됩니다.

기본 StorageGRID 서버 인증서 또는 업로드된 CA 서명 인증서에 대한 자세한 정보를 표시하려면 탭을 선택합니다.



새 인증서를 업로드한 후 관련 인증서 만료 알림(또는 레거시 알림)이 지워지도록 최대 1일을 허용합니다.

5. 페이지를 새로 고쳐 웹 브라우저가 업데이트되도록 합니다.

관련 정보

["S3을 사용합니다"](#)

["Swift를 사용합니다"](#)

["S3 API 엔드포인트 도메인 이름 구성"](#)

S3 및 Swift REST API 엔드포인트에 대한 기본 서버 인증서 복원

S3 및 Swift REST API 엔드포인트에 대한 기본 서버 인증서를 사용하여 로 되돌릴 수 있습니다.

단계

1. 구성 * > * 네트워크 설정 * > * 서버 인증서 * 를 선택합니다.
2. 개체 스토리지 API 서비스 끝점 서버 인증서 섹션에서 * 기본 인증서 사용 * 을 클릭합니다.
3. 확인 대화 상자에서 * 확인 * 을 클릭합니다.

객체 저장소 API 끝점에 대한 기본 서버 인증서를 복원하면 구성된 사용자 지정 서버 인증서 파일이 삭제되고 시스템에서 복구할 수 없습니다. 이후의 모든 새 API 클라이언트 연결에 기본 서버 인증서가 사용됩니다.

4. 페이지를 새로 고쳐 웹 브라우저가 업데이트되도록 합니다.

StorageGRID 시스템의 CA 인증서를 복사하는 중입니다

StorageGRID는 내부 CA(인증 기관)를 사용하여 내부 트래픽을 보호합니다. 인증서를 업로드해도 이 인증서는 변경되지 않습니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.

이 작업에 대해

사용자 지정 서버 인증서가 구성된 경우 클라이언트 응용 프로그램은 사용자 지정 서버 인증서를 사용하여 서버를 확인해야 합니다. StorageGRID 시스템에서 CA 인증서를 복사해서는 안 됩니다.

단계

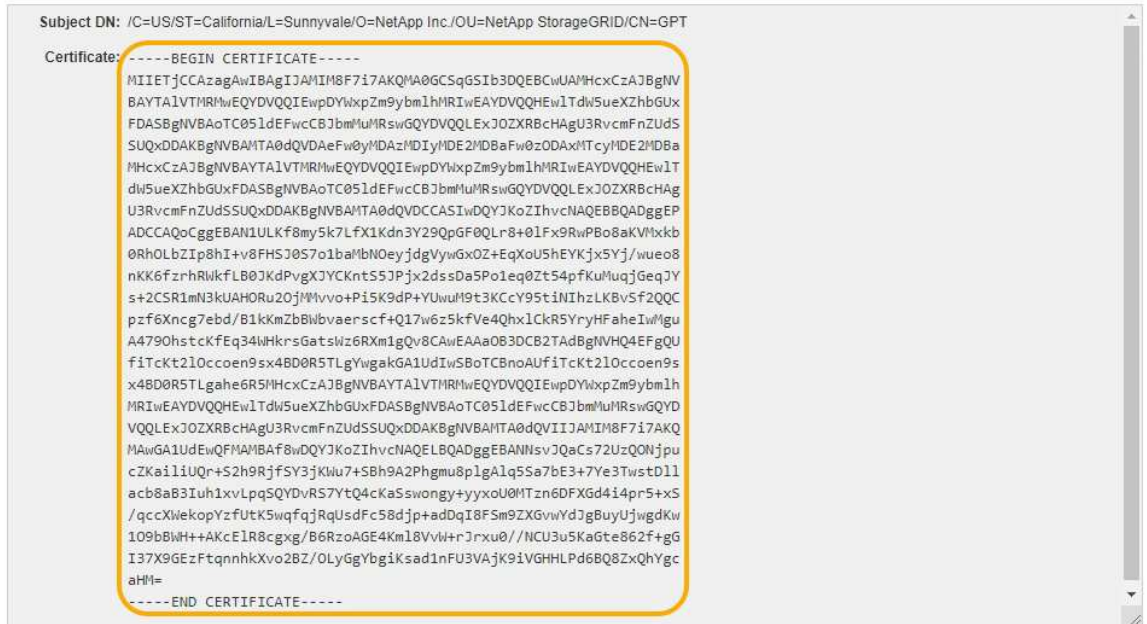
1. 구성 * > * 네트워크 설정 * > * 서버 인증서 * 를 선택합니다.
2. 내부 CA 인증서 * 섹션에서 모든 인증서 텍스트를 선택합니다.

반드시 포함해야 합니다 -----BEGIN CERTIFICATE----- 및 -----END CERTIFICATE----- 선택합니다.

Internal CA Certificate

StorageGRID uses an internal Certificate Authority (CA) to secure internal traffic. This certificate does not change if you upload your own certificates.

To export the internal CA certificate, copy all of the certificate text (starting with -----BEGIN CERTIFICATE and ending with END CERTIFICATE-----), and save it as a .pem file.



3. 선택한 텍스트를 마우스 오른쪽 단추로 클릭하고 * 복사 * 를 선택합니다.
4. 복사한 인증서를 텍스트 편집기에 붙여 넣습니다.
5. 파일을 확장자로 저장합니다 .pem.

예를 들면 다음과 같습니다. storagegrid_certificate.pem

FabricPool용 StorageGRID 인증서 구성

엄격한 호스트 이름 유효성 검사를 수행하고 FabricPool를 사용하는 ONTAP 클라이언트와 같은 엄격한 호스트 이름 유효성 검사를 사용하지 않는 S3 클라이언트의 경우 로드 밸런서 끝점을 구성할 때 서버 인증서를 생성하거나 업로드할 수 있습니다.

필요한 것

- 특정 액세스 권한이 있어야 합니다.
- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.

이 작업에 대해

로드 밸런서 끝점을 만들 때 자체 서명된 서버 인증서를 생성하거나 알려진 CA(인증 기관)에서 서명한 인증서를 업로드할 수 있습니다. 프로덕션 환경에서는 알려진 CA가 서명한 인증서를 사용해야 합니다. CA에서 서명한 인증서는 중단 없이 회전할 수 있습니다. 또한 중간자 공격에 대한 보호 기능이 강화되어 보안이 더욱 강화되고 있습니다.

다음 단계에서는 FabricPool를 사용하는 S3 클라이언트에 대한 일반 지침을 제공합니다. 자세한 내용과 절차는 StorageGRID for FabricPool 구성 지침을 참조하십시오.



게이트웨이 노드의 별도의 CLB(연결 로드 밸런서) 서비스는 더 이상 사용되지 않으며 FabricPool에서 더 이상 사용하지 않는 것이 좋습니다.

단계

1. 선택적으로 FabricPool에서 사용할 고가용성(HA) 그룹을 구성합니다.
2. FabricPool에서 사용할 S3 로드 밸런서 끝점을 만듭니다.

HTTPS 로드 밸런서 끝점을 만들면 서버 인증서, 인증서 개인 키 및 CA 번들을 업로드하라는 메시지가 표시됩니다.

3. StorageGRID을 ONTAP의 클라우드 계층으로 연결

로드 밸런서 끝점 포트와 업로드한 CA 인증서에 사용된 정규화된 도메인 이름을 지정합니다. 그런 다음 CA 인증서를 제공합니다.



중간 CA에서 StorageGRID 인증서를 발급한 경우 중간 CA 인증서를 제공해야 합니다. StorageGRID 인증서가 루트 CA에서 직접 발급된 경우 루트 CA 인증서를 제공해야 합니다.

관련 정보

["FabricPool용 StorageGRID를 구성합니다"](#)

관리 인터페이스에 대해 자체 서명된 서버 인증서를 생성하는 중입니다

스크립트를 사용하여 엄격한 호스트 이름 확인이 필요한 관리 API 클라이언트용 자체 서명된 서버 인증서를 생성할 수 있습니다.

필요한 것

- 특정 액세스 권한이 있어야 합니다.
- 에 가 있어야 합니다 Passwords.txt 파일.

이 작업에 대해

프로덕션 환경에서는 알려진 CA(인증 기관)에서 서명한 인증서를 사용해야 합니다. CA에서 서명한 인증서는 중단 없이 회전할 수 있습니다. 또한 중간자 공격에 대한 보호 기능이 강화되어 보안이 더욱 강화되고 있습니다.

단계

1. 각 관리 노드의 FQDN(정규화된 도메인 이름)을 연습니다.
2. 기본 관리자 노드에 로그인합니다.
 - a. 다음 명령을 입력합니다. `ssh admin@primary_Admin_Node_IP`
 - b. 에 나열된 암호를 입력합니다 Passwords.txt 파일.
 - c. 루트로 전환하려면 다음 명령을 입력합니다. `su -`
 - d. 에 나열된 암호를 입력합니다 Passwords.txt 파일.

루트로 로그인하면 프롬프트가 에서 변경됩니다 \$ 를 선택합니다 #.

3. 자체 서명된 새 인증서를 사용하여 StorageGRID를 구성합니다.

```
$ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
```

- 용 `--domains``에서 와일드카드를 사용하여 모든 관리 노드의 정규화된 도메인 이름을 나타냅니다. 예를 들면, 다음과 같습니다. ``*.ui.storagegrid.example.com` 와일드카드를 사용하여 나타냅니다 `admin1.ui.storagegrid.example.com` 및 `admin2.ui.storagegrid.example.com`.
- 설정 `--type` 를 선택합니다 `management` Grid Manager 및 Tenant Manager에서 사용하는 인증서를 구성합니다.
- 기본적으로 생성된 인증서는 1년(365일) 동안 유효하며 만료되기 전에 다시 만들어야 합니다. 를 사용할 수 있습니다 `--days` 기본 유효 기간을 재정의하는 인수입니다.



인증서의 유효 기간은 언제 시작됩니다 `make-certificate` 가 실행됩니다. 관리 API 클라이언트가 StorageGRID와 동일한 시간 소스와 동기화되어 있는지 확인해야 합니다. 그렇지 않으면 클라이언트가 인증서를 거부할 수 있습니다.

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type management --days 365
```

결과 출력에는 관리 API 클라이언트에 필요한 공용 인증서가 포함됩니다.

4. 인증서를 선택하고 복사합니다.

선택 항목에 BEGIN 및 END 태그를 포함합니다.

5. 명령 셸에서 로그아웃합니다. `$ exit`

6. 인증서가 구성되었는지 확인합니다.

- a. 그리드 관리자에 액세스합니다.
- b. 구성 `** 서버 인증서 * 관리 인터페이스 서버 인증서 *` 를 선택합니다.

7. 복사한 공용 인증서를 사용하도록 관리 API 클라이언트를 구성합니다. BEGIN 및 END Tags를 포함합니다.

스토리지 프록시 설정을 구성하는 중입니다

플랫폼 서비스 또는 클라우드 스토리지 풀을 사용하는 경우 스토리지 노드와 외부 S3 엔드포인트 간에 투명하지 않은 프록시를 구성할 수 있습니다. 예를 들어, 플랫폼 서비스 메시지를 인터넷의 끝점과 같은 외부 끝점으로 보내려면 투명하지 않은 프록시가 필요할 수 있습니다.

필요한 것

- 특정 액세스 권한이 있어야 합니다.
- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.

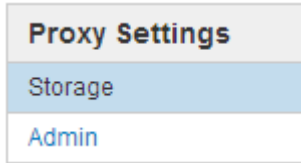
이 작업에 대해

단일 스토리지 프록시에 대한 설정을 구성할 수 있습니다.

단계

1. 구성 * * * 네트워크 설정 * * 프록시 설정 * 을 선택합니다.

스토리지 프록시 설정 페이지가 나타납니다. 기본적으로 보조 아이콘 메뉴에서 * 스토리지 * 가 선택됩니다.



2. 스토리지 프록시 사용 * 확인란을 선택합니다.

스토리지 프록시 구성에 대한 필드가 나타납니다.

Storage Proxy Settings

If you are using platform services or Cloud Storage Pools, you can configure a non-transparent proxy server between Storage Nodes and the external S3 endpoints.

Enable Storage Proxy

Protocol HTTP SOCKS5

Hostname

Port (optional)

3. 투명하지 않은 스토리지 프록시에 대한 프로토콜을 선택합니다.

4. 프록시 서버의 호스트 이름 또는 IP 주소를 입력합니다.

5. 필요에 따라 프록시 서버에 연결하는 데 사용되는 포트를 입력합니다.

프로토콜의 기본 포트(HTTP의 경우 80, SOCKS5의 경우 1080)를 사용하는 경우 이 필드를 비워 둘 수 있습니다.

6. 저장 * 을 클릭합니다.

스토리지 프록시를 저장한 후 플랫폼 서비스 또는 클라우드 스토리지 풀의 새 엔드포인트를 구성 및 테스트할 수 있습니다.



프록시 변경 사항이 적용하려면 최대 10분이 소요될 수 있습니다.

7. 프록시 서버의 설정을 확인하여 StorageGRID의 플랫폼 서비스 관련 메시지가 차단되지 않는지 확인합니다.

작업을 마친 후

스토리지 프록시를 비활성화해야 하는 경우 * 스토리지 프록시 사용 * 확인란의 선택을 취소하고 * 저장 * 을 클릭합니다.

관련 정보

["플랫폼 서비스를 위한 네트워킹 및 포트"](#)

["ILM을 사용하여 개체를 관리합니다"](#)

관리자 프록시 설정을 구성합니다

HTTP 또는 HTTPS를 사용하여 AutoSupport 메시지를 보내는 경우 관리자 노드와 기술 지원(AutoSupport) 간에 투명하지 않은 프록시 서버를 구성할 수 있습니다.

필요한 것

- 특정 액세스 권한이 있어야 합니다.
- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.

이 작업에 대해

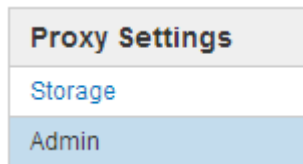
단일 관리 프록시에 대한 설정을 구성할 수 있습니다.

단계

1. 구성 *** 네트워크 설정 ** 프록시 설정 * 을 선택합니다.

관리자 프록시 설정 페이지가 나타납니다. 기본적으로 보조 아이콘 메뉴에서 * 스토리지 * 가 선택됩니다.

2. 측면 표시줄 메뉴에서 * Admin * 을 선택합니다.



3. 관리자 프록시 사용 * 확인란을 선택합니다.

Admin Proxy Settings

If you send AutoSupport messages using HTTPS or HTTP, you can configure a non-transparent proxy server between Admin Nodes and technical support.

Enable Admin Proxy

Hostname

Port

Username (optional)

Password (optional)

4. 프록시 서버의 호스트 이름 또는 IP 주소를 입력합니다.
5. 프록시 서버에 연결하는 데 사용되는 포트를 입력합니다.
6. 필요에 따라 프록시 사용자 이름을 입력합니다.

프록시 서버에 사용자 이름이 필요하지 않은 경우 이 필드를 비워 둡니다.

7. 필요에 따라 프록시 암호를 입력합니다.

프록시 서버에 암호가 필요하지 않은 경우 이 필드를 비워 둡니다.

8. 저장 * 을 클릭합니다.

관리자 프록시가 저장되면 관리 노드와 기술 지원 사이의 프록시 서버가 구성됩니다.



프록시 변경 사항이 적용되려면 최대 10분이 소요될 수 있습니다.

9. 프록시를 비활성화해야 하는 경우 * 관리자 프록시 사용 * 확인란의 선택을 취소하고 * 저장 * 을 클릭합니다.

관련 정보

["AutoSupport 메시지에 대한 프로토콜 지정"](#)

트래픽 분류 정책 관리

서비스 품질(QoS) 오퍼링을 향상하기 위해 트래픽 분류 정책을 생성하여 다양한 유형의 네트워크 트래픽을 식별 및 모니터링할 수 있습니다. 이러한 정책은 트래픽 제한 및 모니터링을 지원할 수 있습니다.

트래픽 분류 정책은 게이트웨이 노드 및 관리 노드에 대한 StorageGRID 로드 밸런서 서비스의 끝점에 적용됩니다. 트래픽 분류 정책을 생성하려면 로드 밸런서 엔드포인트를 이미 생성해야 합니다.

규칙 및 옵션 제한 일치

각 트래픽 분류 정책에는 다음 항목 중 하나 이상에 관련된 네트워크 트래픽을 식별하기 위한 하나 이상의 일치하는 규칙이 포함되어 있습니다.

- 버킷
- 테넌트
- 서브넷(클라이언트가 포함된 IPv4 서브넷)
- 엔드포인트(로드 밸런서 엔드포인트)

StorageGRID는 규칙의 목적에 따라 정책 내의 규칙과 일치하는 트래픽을 모니터링합니다. 정책에 대한 규칙과 일치하는 모든 트래픽은 해당 정책에 의해 처리됩니다. 반대로, 지정된 엔터티를 제외한 모든 트래픽에 일치시키는 규칙을 설정할 수 있습니다.

필요에 따라 다음 매개 변수를 기반으로 정책에 대한 제한을 설정할 수 있습니다.

- 총 대역폭
- 총 대역폭 출력
- 동시 읽기 요청
- 동시 쓰기 요청
- 요청 당 대역폭
- 요청 당 대역폭 출력

- 읽기 요청 속도
- 쓰기 요청 속도



정책을 생성하여 애그리게이트 대역폭을 제한하거나 요청당 대역폭을 제한할 수 있습니다. 그러나 StorageGRID는 두 가지 유형의 대역폭을 동시에 제한할 수 없습니다. 애그리게이트 대역폭 제한은 제한 없는 트래픽에 약간의 성능 영향을 줄 수 있습니다.

트래픽 제한

트래픽 분류 정책을 만들면 설정한 규칙 및 제한 유형에 따라 트래픽이 제한됩니다. 애그리게이트 또는 요청별 대역폭 제한의 경우 요청은 사용자가 설정한 속도로 스트림 인 또는 아웃됩니다. StorageGRID는 단 하나의 속도만 적용할 수 있으므로 가장 구체적인 정책 매칭은 매치 유형별로 적용됩니다. 다른 모든 제한 유형의 경우 클라이언트 요청이 250밀리초 지연되고 일치하는 정책 제한을 초과하는 요청에 대해 503 느린 응답 응답을 수신합니다.

Grid Manager에서 트래픽 차트를 보고 정책이 기대하는 트래픽 제한을 적용하고 있는지 확인할 수 있습니다.

SLA와 함께 트래픽 분류 정책을 사용합니다

용량 제한 및 데이터 보호와 함께 트래픽 분류 정책을 사용하여 용량, 데이터 보호 및 성능에 대한 세부 정보를 제공하는 서비스 수준 계약(SLA)을 적용할 수 있습니다.

트래픽 분류 제한은 부하 분산 장치에 따라 구현됩니다. 트래픽이 여러 부하 분산 장치에 동시에 분산되는 경우 총 최대 속도는 사용자가 지정한 속도 제한의 배수입니다.

다음 예에서는 SLA의 세 가지 계층을 보여 줍니다. 트래픽 분류 정책을 작성하여 각 SLA 계층의 성능 목표를 달성할 수 있습니다.

서비스 수준 계층	용량	데이터 보호	성능	비용
골드	1PB의 스토리지가 허용됩니다	3 ILM 규칙을 복사합니다	초당 25K 요청 5GB/sec(40Gbps) 대역폭	\$\$/월
실버	250TB 저장 가능	2 ILM 규칙을 복사합니다	초당 10K 요청 1.25GB/sec(10Gbps)) 대역폭	\$\$/월
브론즈	100TB 스토리지 허용	2 ILM 규칙을 복사합니다	초당 5K 요청 1 GB/sec(8Gbps) 대역폭	\$/월

트래픽 분류 정책을 생성하는 중입니다

버킷, 테넌트, IP 서브넷 또는 로드 밸런서 끝점별로 네트워크 트래픽을 모니터링하고 선택적으로 제한하려는 경우 트래픽 분류 정책을 생성합니다. 필요에 따라 대역폭, 동시 요청 수 또는 요청 속도를 기준으로 정책에 대한 제한을 설정할 수 있습니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 루트 액세스 권한이 있어야 합니다.
- 일치시킬 로드 밸런서 끝점을 만들어야 합니다.
- 일치시킬 테넌트를 모두 만들어야 합니다.

단계

1. 구성 * > * 네트워크 설정 * > * 트래픽 분류 * 를 선택합니다.

교통 분류 정책 페이지가 나타납니다.

Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.


+ Create	Edit	Remove	Metrics
Name	Description	ID	
<i>No policies found.</i>			

2. Create * 를 클릭합니다.

트래픽 분류 정책 생성 대화 상자가 나타납니다.

Create Traffic Classification Policy

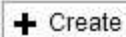


Policy

Name 

Description

Matching Rules

Traffic that matches any rule is included in the policy.

Type	Inverse Match	Match Value
------	---------------	-------------

No matching rules found.

Limits (Optional)

Type	Value	Units
------	-------	-------

No limits found.

Cancel

Save

- 이름 * 필드에 정책의 이름을 입력합니다.

정책을 인식할 수 있도록 설명 이름을 입력합니다.

- 필요에 따라 * Description * (설명 *) 필드에 정책에 대한 설명을 추가합니다.

예를 들어, 이 트래픽 분류 정책이 적용되는 대상 및 제한할 내용에 대해 설명하십시오.

- 정책에 일치하는 규칙을 하나 이상 생성합니다.



일치 규칙은 이 트래픽 분류 정책의 영향을 받을 엔터티를 제어합니다. 예를 들어 특정 테넌트의 네트워크 트래픽에 이 정책을 적용하려면 Tenant를 선택합니다. 또는 이 정책을 특정 로드 밸런싱 장치 끝점의 네트워크 트래픽에 적용하려면 끝점을 선택합니다.


- 일치 규칙 * 섹션에서 * 만들기 * 를 클릭합니다.


일치 규칙 만들기 대화 상자가 나타납니다.


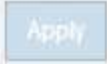
Create Matching Rule

Matching Rules

Type  -- Choose One -- 

Match Value  Choose type before providing match value

Inverse Match 

b. Type * 드롭다운에서 일치하는 규칙에 포함할 요소의 유형을 선택합니다.

c. 일치 값 * 필드에 선택한 요소의 유형에 따라 일치 값을 입력합니다.

- 버킷: 버킷 이름을 입력합니다.

- Bucket Regex: 버킷 이름 집합과 일치시키는 데 사용할 정규식을 입력합니다.

정규식이 고정 해제됩니다. {캐럿} 앵커를 사용하여 버킷 이름의 시작 부분에 일치시키고 \$ 앵커를 사용하여 이름 끝에 일치시킵니다.

- CIDR: 원하는 서브넷과 일치하는 IPv4 서브넷을 CIDR 표기법으로 입력합니다.

- 끝점: 기존 끝점 목록에서 끝점을 선택합니다. 로드 밸런서 엔드포인트 페이지에서 정의한 로드 밸런서 엔드포인트입니다.

- 테넌트: 기존 테넌트 목록에서 테넌트를 선택합니다. 테넌트 일치는 액세스 중인 버킷의 소유권을 기반으로 합니다. 버킷에 대한 익명 액세스는 버킷을 소유하는 테넌트와 일치합니다.

d. 방금 정의한 유형 및 일치 값과 일치하는 모든 `network traffic_except_traffic`을 일치시키려면 * Inverse * 확인란을 선택합니다. 그렇지 않으면 확인란을 선택하지 않은 상태로 둡니다.

예를 들어, 이 정책이 로드 밸런서 끝점 중 하나를 제외한 모든 항목에 적용되도록 하려면 제외할 로드 밸런서 끝점을 지정하고 * Inverse * 를 선택합니다.



하나 이상의 교자가 역마쳐인 여러 마처를 포함하는 정책의 경우 모든 요청과 일치하는 정책을 만들지 않도록 주의하십시오.

e. 적용 * 을 클릭합니다.

규칙이 만들어지고 일치하는 규칙 테이블에 나열됩니다.

+ Create Edit Remove		
Type	Inverse Match	Match Value
• Bucket Regex	✓	control-ld+

Displaying 1 matching rule.

Limits (Optional)

+ Create Edit Remove			
Type	Value	Type	Units
No limits found.			

Cancel Save

a. 정책에 대해 생성할 각 규칙에 대해 이 단계를 반복합니다.

i 모든 규칙과 일치하는 트래픽은 정책에 의해 처리됩니다.

6. 필요에 따라 정책에 대한 제한을 생성합니다.

i 제한을 만들지 않더라도 StorageGRID는 정책과 일치하는 네트워크 트래픽을 모니터링할 수 있도록 메트릭을 수집합니다.

a. Limits * 섹션에서 * Create * 를 클릭합니다.

Create Limit 대화상자가 나타납니다.

Create Limit

Limits (Optional)

Type **?**

Aggregate rate limits in use. Per-request rate limits are not available. **?**

Value **?**

Cancel Apply

b. Type * 드롭다운에서 정책에 적용할 제한 유형을 선택합니다.

다음 목록에서 * in * 은 S3 또는 Swift 클라이언트에서 StorageGRID 로드 밸런서로의 트래픽을 나타내고 *

out * 은 로드 밸런서에서 S3 또는 Swift 클라이언트로 보내는 트래픽을 나타냅니다.

- 총 대역폭
- 총 대역폭 출력
- 동시 읽기 요청
- 동시 쓰기 요청
- 요청 당 대역폭
- 요청 당 대역폭 출력
- 읽기 요청 속도
- 쓰기 요청 속도



정책을 생성하여 애그리게이트 대역폭을 제한하거나 요청당 대역폭을 제한할 수 있습니다. 그러나 StorageGRID는 두 가지 유형의 대역폭을 동시에 제한할 수 없습니다. 애그리게이트 대역폭 제한은 제한 없는 트래픽에 약간의 성능 영향을 줄 수 있습니다.

대역폭 제한에 대해 StorageGRID는 설정된 제한 유형과 가장 일치하는 정책을 적용합니다. 예를 들어, 트래픽을 한 방향으로만 제한하는 정책이 있는 경우 대역폭 제한이 있는 추가 정책과 일치하는 트래픽이 있더라도 반대 방향의 트래픽은 무제한입니다. StorageGRID는 대역폭 제한에 대해 다음 순서로 ""가장 적합한"" 일치 항목을 구현합니다.

- 정확한 IP 주소(/32 마스크)
- 정확한 버킷 이름입니다
- 버킷 regex
- 테넌트
- 엔드포인트
- 일치하지 않는 CIDR 일치(NOT/32)
- 역 일치

c. 값 * 필드에 선택한 제한 유형의 숫자 값을 입력합니다.

한계를 선택하면 예상 단위가 표시됩니다.

d. 적용 * 을 클릭합니다.

제한이 생성되고 Limits 테이블에 나열됩니다.

Type	Inverse Match	Match Value
• Bucket Regex	✓	control-ld+

Displaying 1 matching rule.

Limits (Optional)

Type	Value	Units
• Aggregate Bandwidth Out	10000000000	Bytes/Second

Displaying 1 limit.

Cancel Save

e. 정책에 추가할 각 제한에 대해 이 단계를 반복합니다.

예를 들어, SLA 계층에 대해 40Gbps 대역폭 제한을 생성하려면 한도 내의 총 대역폭 및 총 대역폭 제한을 생성하고 각 대역폭을 40Gbps로 설정합니다.



초당 메가바이트를 초당 기가비트 수로 변환하려면 8을 곱합니다. 예를 들어, 125MB/s는 1,000Mbps 또는 1Gbps와 동일합니다.

7. 규칙 및 제한 만들기를 마치면 * 저장 * 을 클릭합니다.

정책이 저장되고 트래픽 분류 정책 표에 나열됩니다.

Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

Name	Description	ID
• ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574
• Fabric Pools	Monitor Fabric Pools	223b0cbb-6968-4646-b32d-7665bddd894b

Displaying 2 traffic classification policies.

이제 S3 및 Swift 클라이언트 트래픽이 트래픽 분류 정책에 따라 처리됩니다. 트래픽 차트를 보고 정책이 기대하는 트래픽 제한을 적용하고 있는지 확인할 수 있습니다.

관련 정보

["로드 밸런싱 관리"](#)

["네트워크 트래픽 메트릭 보기"](#)

트래픽 분류 정책 편집

트래픽 분류 정책을 편집하여 이름 또는 설명을 변경하거나 정책에 대한 규칙 또는 제한을 생성, 편집 또는 삭제할 수 있습니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 루트 액세스 권한이 있어야 합니다.

단계

1. 구성 * > * 네트워크 설정 * > * 트래픽 분류 * 를 선택합니다.

트래픽 분류 정책 페이지가 나타나고 기존 정책이 표에 나열됩니다.

Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

+ Create	✎ Edit	✕ Remove	📊 Metrics
Name	Description	ID	
<input type="radio"/> ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574	
<input checked="" type="radio"/> Fabric Pools	Monitor Fabric Pools	223b0cbb-6968-4646-b32d-7665bdc894b	


Displaying 2 traffic classification policies.

2. 편집할 정책 왼쪽의 라디오 버튼을 선택합니다.
3. 편집 * 을 클릭합니다.

트래픽 분류 정책 편집 대화 상자가 나타납니다.

Edit Traffic Classification Policy "Fabric Pools"

Policy

Name 

Fabric Pools

Description (optional)

Monitor Fabric Pools

Matching Rules

Traffic that matches any rule is included in the policy.

 Create	 Edit	 Remove
Type	Inverse Match	Match Value
<input checked="" type="checkbox"/> CIDR		10.10.152.0/24
Displaying 1 matching rule.		

Limits (Optional)

 Create	 Edit	 Remove
Type	Value	Units
No limits found.		

Cancel

Save

- 필요에 따라 일치하는 규칙 및 제한을 생성, 편집 또는 제거합니다.
 - 일치하는 규칙 또는 제한을 만들려면 * 만들기 * 를 클릭하고 규칙을 만들거나 제한을 만드는 방법에 대한 지침을 따릅니다.
 - 일치하는 규칙 또는 제한을 편집하려면 규칙 또는 제한에 대한 라디오 단추를 선택하고 * 일치 규칙 * 섹션 또는 * 제한 * 섹션에서 * 편집 * 을 클릭한 다음 규칙 만들기 또는 제한 만들기 지침을 따릅니다.
 - 일치하는 규칙 또는 제한을 제거하려면 규칙 또는 제한에 대한 라디오 단추를 선택하고 * 제거 * 를 클릭합니다. 그런 다음 * 확인 * 을 클릭하여 규칙 또는 제한을 제거할 것인지 확인합니다.
- 규칙 또는 제한을 만들거나 편집한 후에는 * 적용 * 을 클릭합니다.
- 정책 편집이 완료되면 * 저장 * 을 클릭합니다.

정책 변경 사항이 저장되고 이제 트래픽 분류 정책에 따라 네트워크 트래픽이 처리됩니다. 트래픽 차트를 보고 정책이 기대하는 트래픽 제한을 적용하고 있는지 확인할 수 있습니다.

트래픽 분류 정책을 삭제하는 중입니다

트래픽 분류 정책이 더 이상 필요하지 않으면 삭제할 수 있습니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 루트 액세스 권한이 있어야 합니다.

단계

1. 구성 * > * 네트워크 설정 * > * 트래픽 분류 * 를 선택합니다.

트래픽 분류 정책 페이지가 나타나고 기존 정책이 표에 나열됩니다.

Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

Name	Description	ID
<input type="radio"/> ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574
<input checked="" type="radio"/> Fabric Pools	Monitor Fabric Pools	223b0cbb-6968-4646-b32d-7665bddc894b

Displaying 2 traffic classification policies.

2. 삭제할 정책의 왼쪽에 있는 라디오 버튼을 선택합니다.
3. 제거 * 를 클릭합니다.

경고 대화 상자가 나타납니다.



4. 확인 * 을 클릭하여 정책 삭제를 확인합니다.

정책이 삭제됩니다.

네트워크 트래픽 메트릭 보기

트래픽 분류 정책 페이지에서 사용할 수 있는 그래프를 보고 네트워크 트래픽을 모니터링할 수 있습니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 루트 액세스 권한이 있어야 합니다.

이 작업에 대해

기존 트래픽 분류 정책에 대해 로드 밸런서 서비스에 대한 메트릭을 확인하여 정책이 네트워크 전체의 트래픽을 성공적으로 제한하고 있는지 확인할 수 있습니다. 그래프의 데이터를 통해 정책을 조정해야 하는지 확인할 수 있습니다.

트래픽 분류 정책에 대해 설정된 제한이 없더라도 메트릭이 수집되고 그래프는 트래픽 추세를 이해하는 데 유용한 정보를 제공합니다.

단계

1. 구성 * > * 네트워크 설정 * > * 트래픽 분류 * 를 선택합니다.

트래픽 분류 정책 페이지가 나타나고 기존 정책이 표에 나열됩니다.

Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

+ Create ✎ Edit ✕ Remove 📊 Metrics		
Name	Description	ID
<input type="radio"/> ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574
<input checked="" type="radio"/> Fabric Pools	Monitor Fabric Pools	223b0cbb-6968-4646-b32d-7665bddc894b

Displaying 2 traffic classification policies.

2. 메트릭을 보려는 정책 왼쪽의 라디오 버튼을 선택합니다.
3. 메트릭 * 을 클릭합니다.

새 브라우저 창이 열리고 트래픽 분류 정책 그래프가 나타납니다. 그래프에는 선택한 정책과 일치하는 트래픽에 대한 메트릭만 표시됩니다.

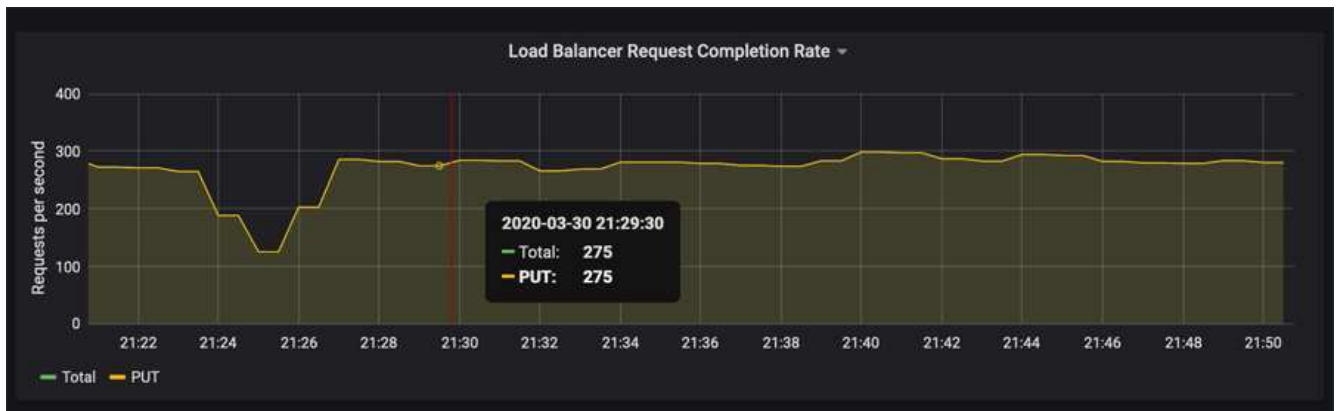
policy * 폴다운을 사용하여 확인할 다른 정책을 선택할 수 있습니다.



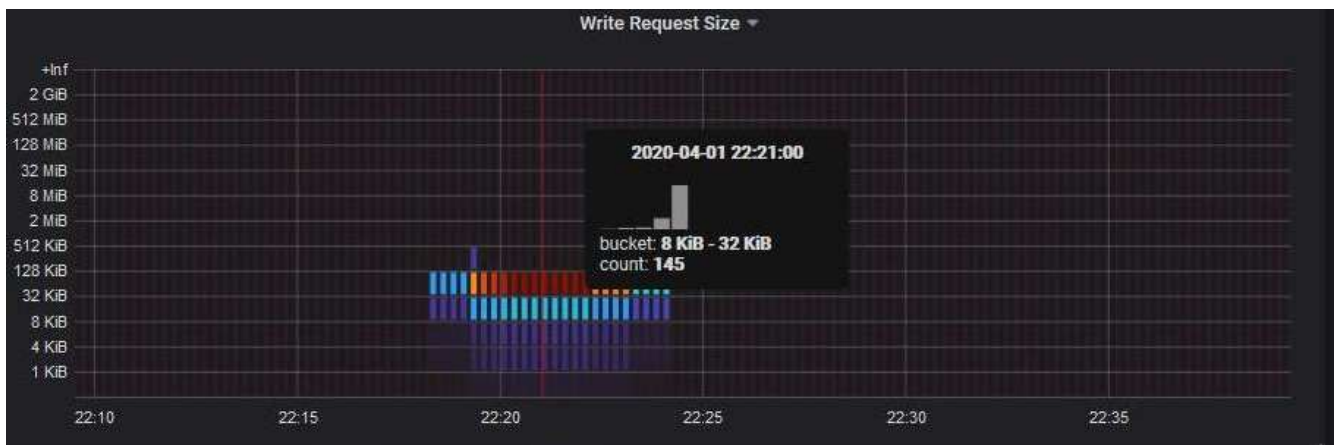
다음 그래프는 웹 페이지에 포함되어 있습니다.

- 로드 밸런서 요청 트래픽: 이 그래프는 로드 밸런서 끝점과 요청을 하는 클라이언트 간에 전송되는 데이터 처리량의 3분 이동 평균을 초당 비트 수로 제공합니다.
- 부하 분산 요청 완료율: 이 그래프는 초당 완료된 요청 수(GET, PUT, HEAD 및 DELETE)에 대한 3분의 이동 평균을 요청 유형별로 제공합니다. 이 값은 새 요청의 헤더가 검증되면 업데이트됩니다.
- 오류 응답 속도: 이 그래프는 오류 응답 코드로 분리된 초당 클라이언트에 반환된 오류 응답 수의 이동 평균을 3분으로 제공합니다.
- 평균 요청 기간(오류 없음): 이 그래프는 요청 유형(GET, PUT, HEAD, DELETE)별로 분류되는 요청 지속 시간의 3분 이동 평균을 제공합니다. 각 요청 기간은 부하 분산 서비스에서 요청 헤더를 구문 분석할 때 시작되어 완전한 응답 본문이 클라이언트로 반환될 때 종료됩니다.
- 개체 크기별 쓰기 요청 속도: 이 히트맵은 개체 크기에 따라 쓰기 요청이 완료되는 속도의 이동 평균을 3분으로 제공합니다. 이 컨텍스트에서 쓰기 요청은 PUT 요청에만 참조됩니다.
- 개체 크기별 읽기 요청 속도: 이 히트맵은 개체 크기에 따라 읽기 요청이 완료되는 속도에 대한 3분의 이동 평균을 제공합니다. 이 컨텍스트에서 읽기 요청은 요청 가져오기만 참조합니다. 히트맵의 색상은 개별 그래프 내의 개체 크기의 상대적 주파수를 나타냅니다. 차가운 색(예: 자주색 및 파란색)은 상대적으로 낮은 비율을 나타내고 따뜻한 색(예: 주황색 및 빨간색)은 상대적으로 높은 비율을 나타냅니다.

4. 커서를 선 그래프 위로 이동하면 그래프의 특정 부분에 있는 값의 팝업이 표시됩니다.



5. Heatmap 위로 커서를 이동하면 샘플의 날짜 및 시간, 카운트로 집계된 개체 크기 및 해당 기간 동안 초당 요청 수를 보여주는 팝업이 표시됩니다.



6. 왼쪽 상단의 * 정책 * 폴다운을 사용하여 다른 정책을 선택합니다.

선택한 정책에 대한 그래프가 나타납니다.

7. 또는 * Support * (지원 *) 메뉴에서 그래프에 액세스하십시오.
 - a. 지원 * > * 도구 * > * 메트릭 * 을 선택합니다.
 - b. 페이지의 * Grafana * 섹션에서 * 트래픽 분류 정책 * 을 선택합니다.
 - c. 페이지 왼쪽 상단의 풀다운 메뉴에서 정책을 선택합니다.

트래픽 분류 정책은 ID로 식별됩니다. 정책 ID는 트래픽 분류 정책 페이지에 나열되어 있습니다.

8. 그래프를 분석하여 정책에 따라 트래픽이 제한되는 빈도와 정책을 조정해야 하는지 여부를 결정합니다.

관련 정보

["모니터링 및 문제 해결"](#)

링크 비용은 얼마입니까

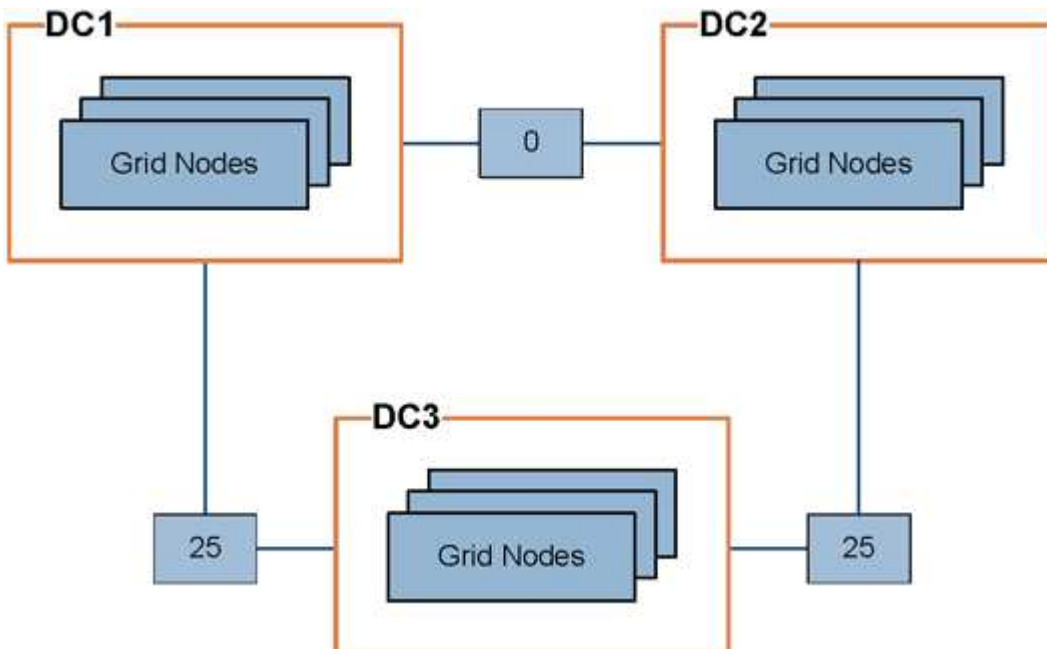
링크 비용을 사용하면 둘 이상의 데이터 센터 사이트가 있을 때 요청된 서비스를 제공하는 데이터 센터 사이트의 우선 순위를 지정할 수 있습니다. 링크 비용을 조정하여 사이트 간 지연 시간을 반영할 수 있습니다.

- 링크 비용은 오브젝트 검색을 수행하는 데 사용되는 오브젝트 복사본의 우선 순위를 지정하는 데 사용됩니다.
- 링크 비용은 그리드 관리 API 및 테넌트 관리 API에서 사용할 내부 StorageGRID 서비스를 결정하는 데 사용됩니다.
- 링크 비용은 게이트웨이 노드의 CLB 서비스에서 클라이언트 연결을 연결하는 데 사용됩니다.



CLB 서비스는 더 이상 사용되지 않습니다.

다이어그램에는 사이트 간에 구성된 링크 비용이 있는 세 개의 사이트 표가 표시됩니다.



- 게이트웨이 노드의 CLB 서비스는 동일한 데이터 센터 사이트의 모든 스토리지 노드 및 링크 비용이 0인 모든

데이터 센터 사이트에 클라이언트 연결을 균등하게 분산합니다.

이 예에서는 데이터 센터 사이트 1(DC1)의 게이트웨이 노드가 DC1의 스토리지 노드 및 DC2의 스토리지 노드로 클라이언트 접속을 균등하게 분산합니다. DC3의 게이트웨이 노드는 DC3의 스토리지 노드에만 클라이언트 접속을 전송합니다.

- 여러 개의 복제된 복제본으로 존재하는 객체를 검색할 때 StorageGRID는 가장 낮은 링크 비용을 가진 데이터 센터에서 복제본을 검색합니다.

이 예제에서 DC2의 클라이언트 응용 프로그램이 DC1과 DC3에 둘 다 저장된 객체를 검색할 경우 DC1에서 D2까지의 링크 비용은 DC3에서 DC2로 링크 비용보다 낮은 0이므로 DC2의 클라이언트 응용 프로그램이 DC1에서 객체를 검색합니다.

링크 비용은 특정 측정 단위가 없는 임의의 상대 숫자입니다. 예를 들어 링크 비용 50은 링크 비용 25보다 우선적으로 사용됩니다. 이 표에는 일반적으로 사용되는 링크 비용이 나와 있습니다.

링크	링크 비용	참고
데이터를 안전하게 보호	25(기본값)	WAN 링크로 연결된 데이터 센터
동일한 물리적 위치의 논리적 데이터 센터 사이트 간	0	LAN으로 연결된 동일한 물리적 건물 또는 캠퍼스의 논리적 데이터 센터

관련 정보

["로드 균형 조정 작동 방식 - CLB 서비스"](#)

링크 비용을 업데이트하는 중입니다

사이트 간 지연 시간을 반영하기 위해 데이터 센터 사이트 간의 링크 비용을 업데이트할 수 있습니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 그리드 토폴로지 페이지 구성 권한이 있어야 합니다.


단계



1. 구성 * > * 네트워크 설정 * > * 링크 비용 * 을 선택합니다.



Link Cost

Updated: 2021-03-29 12:28:41 EDT


Site Names (1 - 2 of 2) 

Site ID	Site Name	Actions
10	Data Center 1	
20	Data Center 2	

Show Records Per Page Previous « 1 » Next


Link Costs

Link Source	Link Destination	Actions
<input type="text" value="10"/>	<input type="text" value="20"/>	

Apply Changes 

2. 링크 원본 * 에서 사이트를 선택하고 * 링크 대상 * 에서 0에서 100 사이의 비용 값을 입력합니다.

소스가 대상과 동일한 경우 링크 비용을 변경할 수 없습니다.

변경 사항을 취소하려면  를 클릭합니다 * 되돌리기 *.

3. 변경 내용 적용 * 을 클릭합니다.

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.